AMENDMENTS to the SPECIFICATION

Please amend the ABSTRACT to read as follows:

[0097] ~~A client device authenticated a one-time pad table stored in the client device, and a matching table maintained by a service provider. When a request for service is posted from the client to the service provider, the next unused pad is exchanged and verified with the current state of the service provider's copy of the table. If the OTP is the next unused code, service is granted, else the user is challenged to identify himself, which when successfully completed results in the client device being downloaded with a new OTP table, replacing the compromised table. Use of service by a cloned device causes the OTP table at the service provider to become out of synchronization with the authentic device's copy of the table, thereby setting up the ability to detect the fraud, stop the service consumption by the clone, and reprogram the authentic device to allow for uninterrupted service.~~ Authentication of cellular telephone device by providing a first one-time pad cryptological table to a security server which has multiple sequenced One Time Pad value entries including a previous use indicator initialized as"unused", and providing a second one-time pad cryptological table to an authentic device initially synchronized with the first table. A cloned copy of the second table is stored in an inauthentic cellular telephone device, these third table being initially synchronized with the second table. The authentic device selects an unused entry in the second table and transmits it to the server when requesting service. If the received entry matches a next sequential unused entry in the first table, the server grants service, and both server and authentic device mark that entry as used. If the received entry does not match a sequentially next unused entry in the first table, service is denied to the requesting device.

Please amend paragraph [0041] to read as follows:

[0041] ~~The present invention provides an exclusive method to solve cell phone cloning cases. Our new solution uses a combination of technologies to combat theft and fraudulent billing through rapid detection of a cloned device accessing services. In addition, our method can significantly reduce service billing usage from cloned devices, thereby discouraging and reducing illegal cloning activities.~~ Authentication of cellular telephone device is accomplished by providing a first one-time pad cryptological table to a security server which has multiple sequenced One Time Pad value entries including a previous use indicator initialized as"unused", and providing a second one-time pad cryptological table to an authentic device initially synchronized with the first table. A cloned copy of the second table is stored in an inauthentic cellular telephone device, these third table being initially synchronized with the second table. The authentic device selects an unused entry in the second table and transmits it to the server when requesting service. If the received entry matches a next sequential unused entry in the first table, the server grants service, and both server and authentic device mark that entry as used. If the received entry does not match a sequentially next unused entry in the first table, service is denied to the requesting device.

Please delete paragraphs [0042] - [0043].